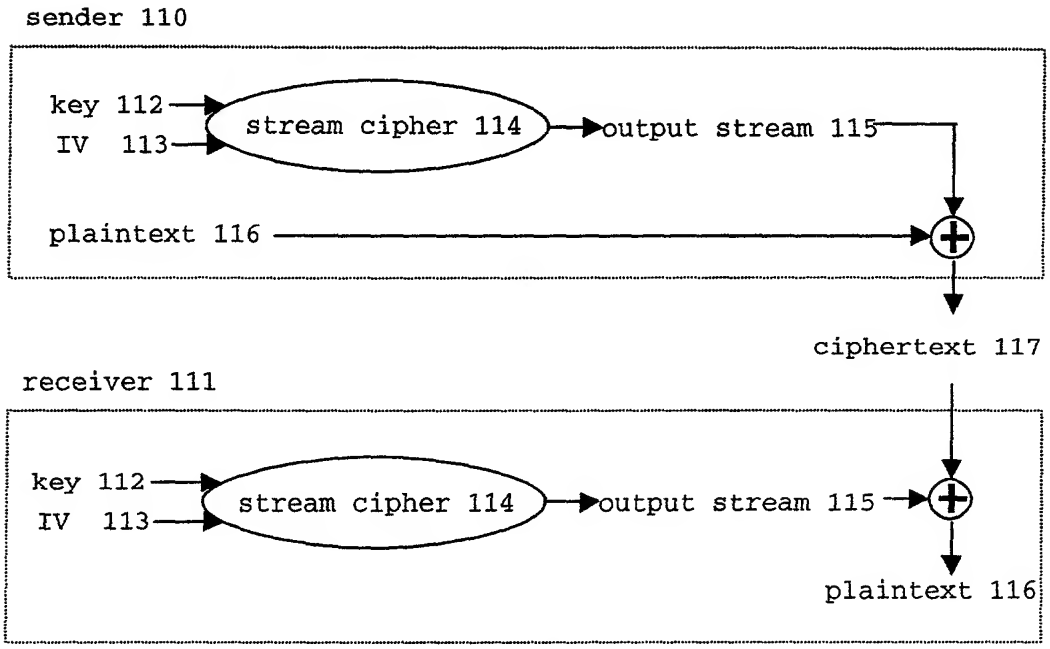


Figure. 1. Typical usage of a stream cipher
PRIOR ART

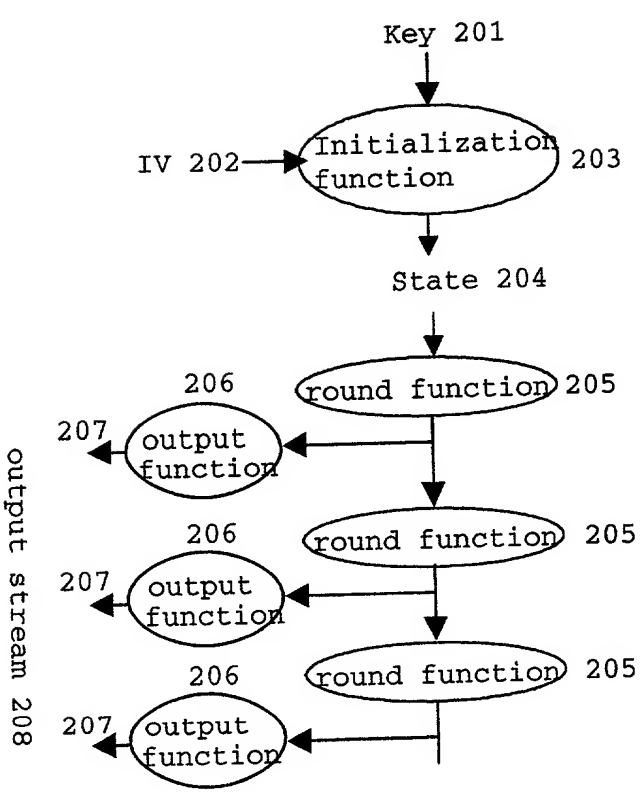


Figure 2. Structure of a typical stream cipher
PRIOR ART

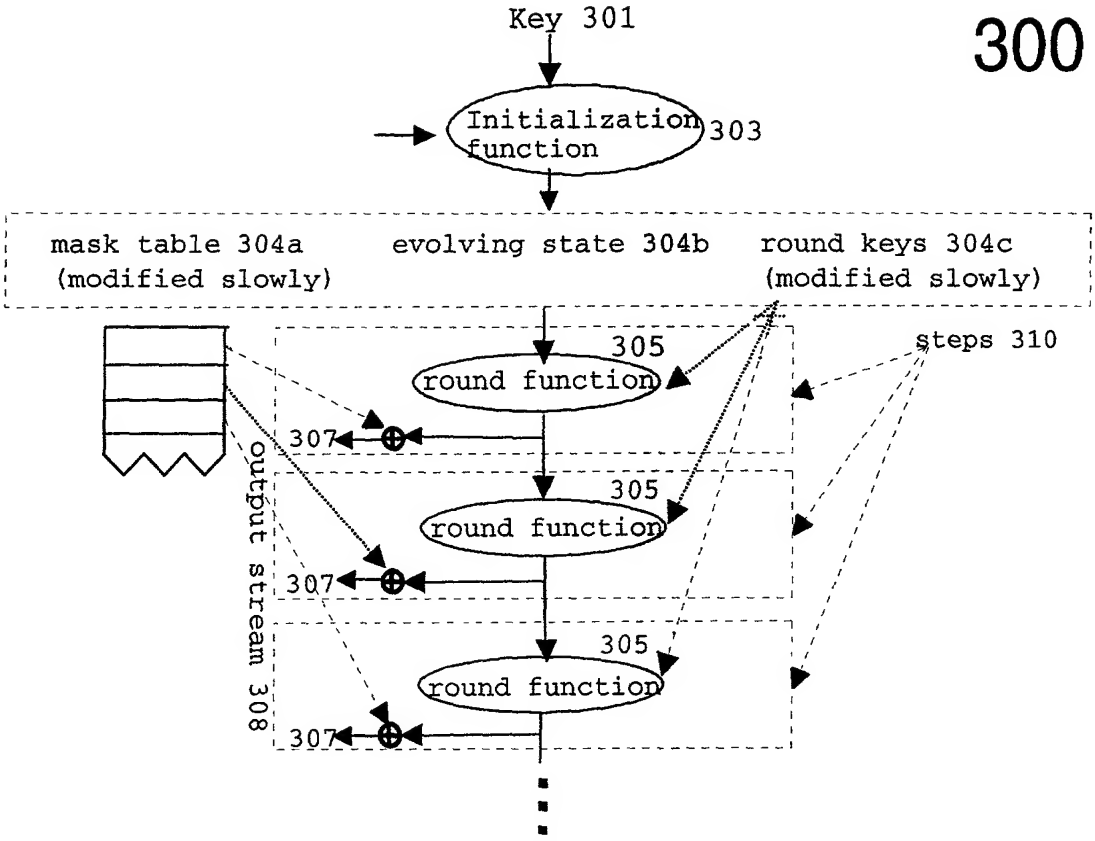


Figure 3

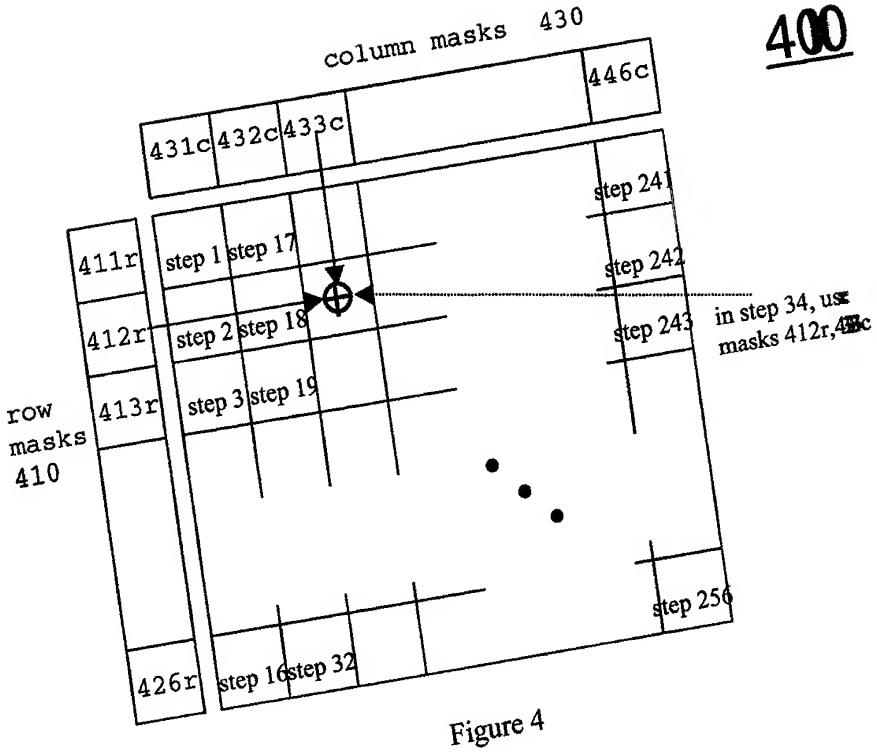


Figure 4

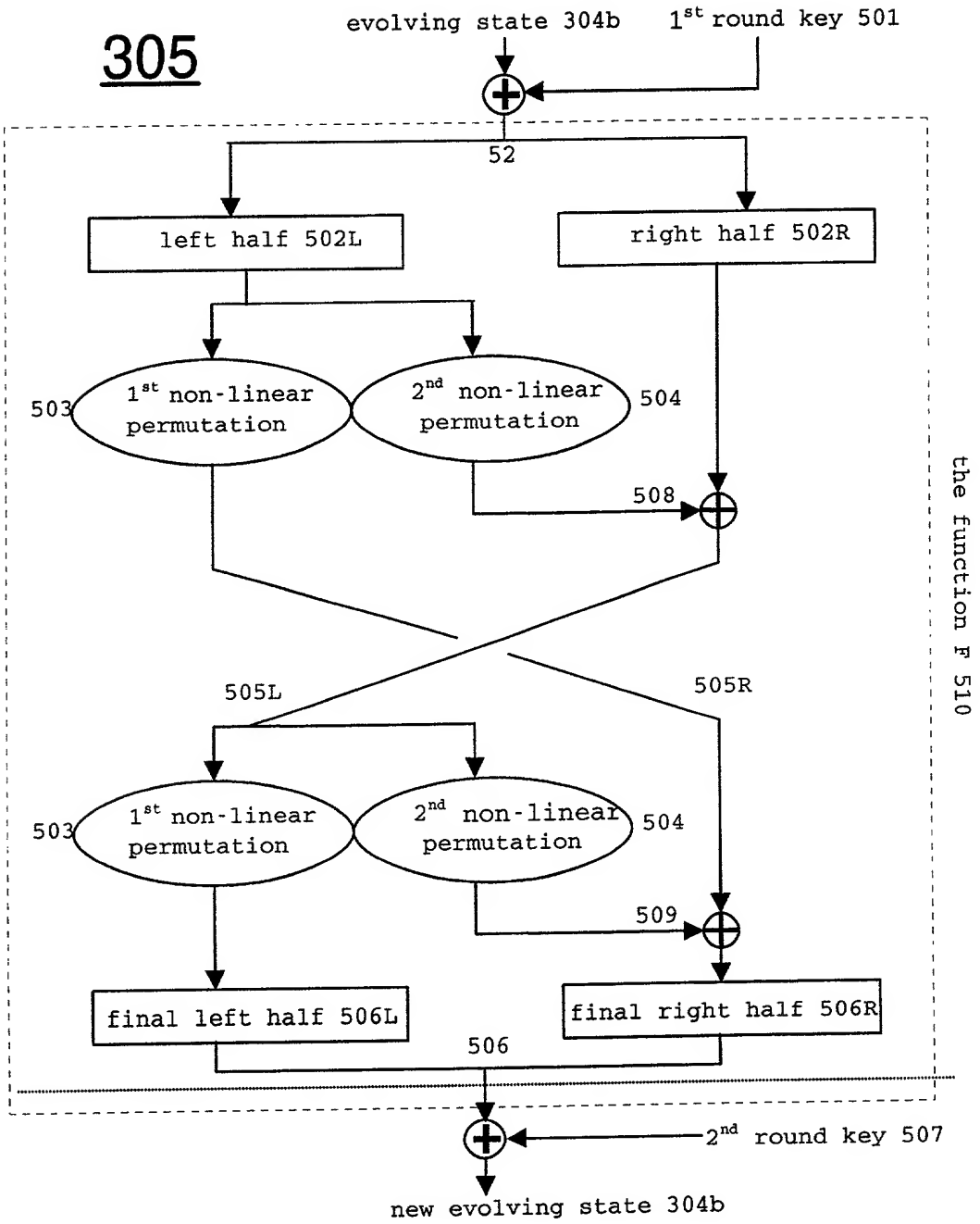

305
evolving state 304b
1st round key 501
52
left half 502L
right half 502R
503
1st non-linear permutation
2nd non-linear permutation
504
508
505L
505R
503
1st non-linear permutation
2nd non-linear permutation
504
509
final left half 506L
final right half 506R
506
2nd round key 507
new evolving state 304b
the function F 510

Figure 5

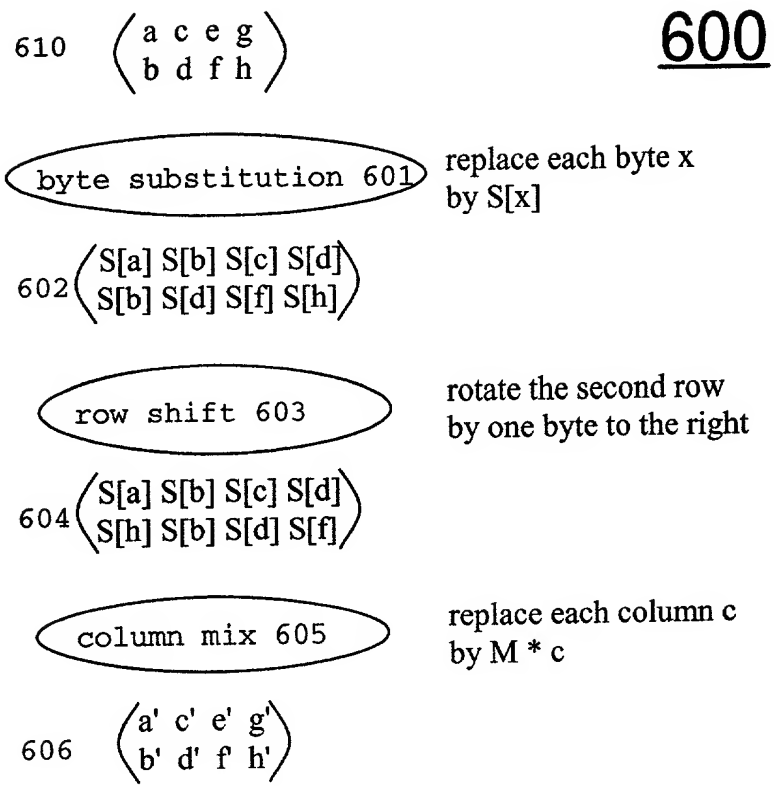
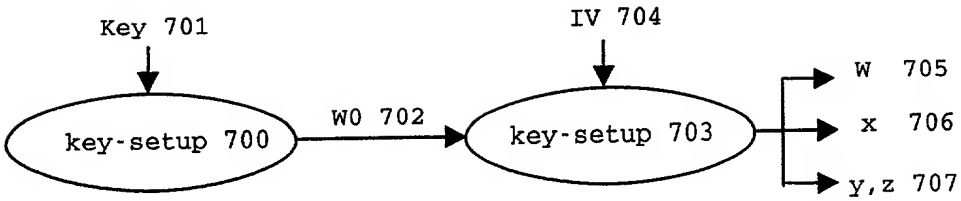

600
610
a c e g
b d f h
byte substitution 601
replace each byte x
by S[x]
602
S[a] S[b] S[c] S[d]
S[b] S[d] S[f] S[h]
row shift 603
rotate the second row
by one byte to the right
604
S[a] S[b] S[c] S[d]
S[h] S[b] S[d] S[f]
column mix 605
replace each column c
by M * c
606
a' c' e' g'
b' d' f' h'

Figure 6



202, 302 Figure 7